(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 November 2005 (10.11.2005)

PCT

(10) International Publication Number
WO 2005/107144 A1

(51) International Patent Classification[7]: H04L 9/32, 12/22, H04Q 7/20

(21) International Application Number:
PCT/CA2005/000652

(22) International Filing Date: 29 April 2005 (29.04.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/567,293 30 April 2004 (30.04.2004) US

(71) Applicant *(for all designated States except US)*: **RESEARCH IN MOTION LIMITED** [CA/CA]; 295 Phillip Street, Waterloo, Ontario N2L 3W8 (CA).

(72) Inventors: **ADAMS, Neil, P.**; 550 Little Dover Cres., Waterloo, Ontario N2K 4E4 (CA). **LITTLE, Herbert, A.**; 504 Old Oak Place, Waterloo, Ontario N2T 2V8 (CA). **KIRKUP, Michael, G.**; 413 Exmoor Street, Waterloo, Ontario N2K 3X5 (CA).

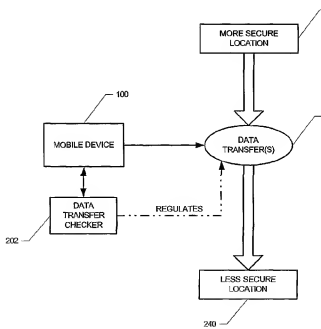
(74) Agents: **WONG, Jeffrey, W.** et al.; Borden Ladner Gervais LLP, 100 Queen Street, Suite 1100, Ottawa, Ontario K1P 1J0 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR HANDLING DATA TRANSFERS



(57) Abstract: A system, method, and apparatus for managing data transfers between a secure location and a less secure location based on data transfer settings established by an administrator and according to security related aspects and business policy requirements are presented. A data transfer checker apparatus stored and operating on a wireless mobile device retrieves data transfer settings to determine if requested data to be transferred from a first location to a second location is to be performed.

WO 2005/107144 A1

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR HANDLING DATA TRANSFERS

BACKGROUND

Technical Field

This document relates generally to the field of communications, and in particular to handling data transfers that involve mobile wireless communications devices.

Description of the Related Art

Some companies or governments have different types of networks based on different levels of security. Some of the networks are more secure than others and provide additional levels of security, as well as different procedures for using that network. It is a security concern for data to move between the networks, specifically from a more secure network to a weaker network. An additional problem is how to prevent a malicious application from siphoning data from inside a corporation's firewall to outside the firewall.

For example the government may have a secret network and a non-secret network. The workstations on the secret network may not even be connected to the non-secret network to explicitly prevent data siphoning. To prevent data siphoning between these networks for mobile communications, the government would have to deploy two separate PDAs to each employee that uses both of the networks. This is a costly approach.

As another example, an organization may wish to deploy handhelds to employees, which connect to their corporate network as well as their personal (home) email accounts. It would be detrimental for an employee to siphon data between their corporate secure network to their personal accounts.

SUMMARY

In accordance with the teachings disclosed herein, systems and methods are provided for managing data transfers between a secure location and a less secure location. As an example of a system and method, a data transfer checker operating on a mobile device determines whether an attempted data transfer between two locations is permitted. If it is not permitted, then the data transfer is prevented and the user may be notified of the data transfer prevention.

As another example of a system and method, a system and method can receive a data transfer request to transfer data from a first location to a second location, wherein the

first location is more secure than the second location. Data transfer settings are retrieved from a data store responsive to receiving the data transfer request. The data transfer settings indicate whether a data transfer is to occur based upon a security-related aspect associated with the data transfer. The data transfer settings are used to determine whether to transfer the data from the first location to the second location based upon the data transfer settings. The data is transferred responsive to the determining step.

A system and method may be configured to consider one or more different data transfer security-related aspects, such as level of security associated with the destination of the data transfer. As other examples, a security related aspect can include the type of communication operation to be performed between the first location and the second location such as the type of communication to occur. The type of data transfer operation could include data forwarding between service books, opening an internal and an external connection, an Inter-Process Communication (IPC) between applications, and/or a cut-copy-paste type operation between applications.

As will be appreciated, the systems and methods described herein are capable of many different embodiments, and are capable of modifications in various respects

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is an overview of an example communication system in which a wireless communication device may be used.

FIG. 2 is a block diagram of a further example communication system including multiple networks and multiple mobile communication devices.

FIGS. 3 and 4 are block diagrams depicting management of data transfers between a secure location and a less secure location.

FIG. 5 is a block diagram depicting an IT administrator providing data transfer settings to a mobile device.

FIGS. 6 and 7 are flowcharts depicting a data transfer operational scenario.

FIG. 8 is a block diagram depicting a data transfer prevention feature wherein data forwarding between service books is prevented.

FIG. 9 is a block diagram depicting a data transfer prevention feature wherein cut/copy/paste operations are disabled for applications on a mobile device.

FIG. 10 is a block diagram depicting a data transfer prevention feature wherein Inter-Process Communication (IPC) are disabled between applications operating on a mobile device.

FIG. 11 is a block diagram of an example mobile device.

DETAILED DESCRIPTION OF THE DRAWINGS

FIG. 1 is an overview of an example communication system in which a wireless communication device may be used. One skilled in the art will appreciate that there may be many different topologies, but the system shown in FIG. 1 helps demonstrate the operation of the encoded message processing systems and methods described in the present application. There may also be many message senders and recipients. The simple system shown in FIG. 1 is for illustrative purposes only, and shows perhaps the most prevalent Internet e-mail environment where security is not generally used.

FIG. 1 shows an e-mail sender 10, the Internet 20, a message server system 40, a wireless gateway 85, wireless infrastructure 90, a wireless network 105 and a mobile communication device 100.

An e-mail sender system 10 may, for example, be connected to an ISP (Internet Service Provider) on which a user of the system 10 has an account, located within a company, possibly connected to a local area network (LAN), and connected to the Internet 20, or connected to the Internet 20 through a large ASP (application service provider) such as America Online (AOL). Those skilled in the art will appreciate that the systems shown in FIG. 1 may instead be connected to a wide area network (WAN) other than the Internet, although e-mail transfers are commonly accomplished through Internet-connected arrangements as shown in FIG. 1.

The message server 40 may be implemented, for example, on a network computer within the firewall of a corporation, a computer within an ISP or ASP system or the like, and acts as the main interface for e-mail exchange over the Internet 20. Although other messaging systems might not require a message server system 40, a mobile device 100 configured for receiving and possibly sending e-mail will normally be associated with an account on a message server. Perhaps the two most common message servers are Microsoft Exchange™ and Lotus Domino™. These products are often used in conjunction with Internet mail routers that route and deliver mail. These intermediate components are not shown in FIG. 1, as they do not directly play a role in the secure

message processing described below. Message servers such as server 40 typically extend beyond just e-mail sending and receiving; they also include dynamic database storage engines that have predefined database formats for data like calendars, to-do lists, task lists, e-mail and documentation.

The wireless gateway 85 and infrastructure 90 provide a link between the Internet 20 and wireless network 105. The wireless infrastructure 90 determines the most likely network for locating a given user and tracks the user as they roam between countries or networks. A message is then delivered to the mobile device 100 via wireless transmission, typically at a radio frequency (RF), from a base station in the wireless network 105 to the mobile device 100. The particular network 105 may be virtually any wireless network over which messages may be exchanged with a mobile communication device.

As shown in FIG. 1, a composed e-mail message 15 is sent by the e-mail sender 10, located somewhere on the Internet 20. This message 15 is normally fully in the clear and uses traditional Simple Mail Transfer Protocol (SMTP), RFC822 headers and Multipurpose Internet Mail Extension (MIME) body parts to define the format of the mail message. These techniques are all well known to those skilled in the art. The message 15 arrives at the message server 40 and is normally stored in a message store. Most known messaging systems support a so-called "pull" message access scheme, wherein the mobile device 100 must request that stored messages be forwarded by the message server to the mobile device 100. Some systems provide for automatic routing of such messages which are addressed using a specific e-mail address associated with the mobile device 100. In a preferred embodiment described in further detail below, messages addressed to a message server account associated with a host system such as a home computer or office computer which belongs to the user of a mobile device 100 are redirected from the message server 40 to the mobile device 100 as they are received.

Regardless of the specific mechanism controlling the forwarding of messages to the mobile device 100, the message 15, or possibly a translated or reformatted version thereof, is sent to the wireless gateway 85. The wireless infrastructure 90 includes a series of connections to wireless network 105. These connections could be Integrated Services Digital Network (ISDN), Frame Relay or T1 connections using the TCP/IP protocol used throughout the Internet. As used herein, the term "wireless network" is intended to include three different types of networks, those being (1) data-centric wireless networks, (2) voice-centric wireless networks and (3) dual-mode networks that can support both voice and data

communications over the same physical base stations. Combined dual-mode networks include, but are not limited to, (1) Code Division Multiple Access (CDMA) networks, (2) the Groupe Special Mobile or the Global System for Mobile Communications (GSM) and the General Packet Radio Service (GPRS) networks, and (3) future third-generation (3G) networks like Enhanced Data-rates for Global Evolution (EDGE) and Universal Mobile Telecommunications Systems (UMTS). Some older examples of data-centric network include the Mobitex™ Radio Network and the DataTAC™ Radio Network. Examples of older voice-centric data networks include Personal Communication Systems (PCS) networks like GSM, and TDMA systems.

FIG. 2 is a block diagram of a further example communication system including multiple networks and multiple mobile communication devices. The system of FIG. 2 is substantially similar to the FIG. 1 system, but includes a host system 30, a redirection program 45, a mobile device cradle 65, a wireless virtual private network (VPN) router 75, an additional wireless network 110 and multiple mobile communication devices 100. As described above in conjunction with FIG. 1, FIG. 2 represents an overview of a sample network topology. Although the encoded message processing systems and methods described herein may be applied to networks having many different topologies, the network of FIG. 2 is useful in understanding an automatic e-mail redirection system mentioned briefly above.

The central host system 30 will typically be a corporate office or other LAN, but may instead be a home office computer or some other private system where mail messages are being exchanged. Within the host system 30 is the message server 40, running on some computer within the firewall of the host system, that acts as the main interface for the host system to exchange e-mail with the Internet 20. In the system of FIG. 2, the redirection program 45 enables redirection of data items from the server 40 to a mobile communication device 100. Although the redirection program 45 is shown to reside on the same machine as the message server 40 for ease of presentation, there is no requirement that it must reside on the message server. The redirection program 45 and the message server 40 are designed to co-operate and interact to allow the pushing of information to mobile devices 100. In this installation, the redirection program 45 takes confidential and non-confidential corporate information for a specific user and redirects it out through the corporate firewall to mobile devices 100. A more detailed description of the redirection software 45 may be found in the commonly assigned United States Patent

6,219,694 ("the '694 Patent"), entitled "System and Method for Pushing Information From A Host System To A Mobile Data Communication Device Having A Shared Electronic Address", and issued to the assignee of the instant application on April 17, 2001. This push technique may use a wireless friendly encoding, compression and encryption technique to deliver all information to a mobile device, thus effectively extending the security firewall to include each mobile device 100 associated with the host system 30.

As shown in FIG. 2, there may be many alternative paths for getting information to the mobile device 100. One method for loading information onto the mobile device 100 is through a port designated 50, using a device cradle 65. This method tends to be useful for bulk information updates often performed at initialization of a mobile device 100 with the host system 30 or a computer 35 within the system 30. The other main method for data exchange is over-the-air using wireless networks to deliver the information. As shown in FIG. 2, this may be accomplished through a wireless VPN router 75 or through a traditional Internet connection 95 to a wireless gateway 85 and a wireless infrastructure 90, as described above. The concept of a wireless VPN router 75 is new in the wireless industry and implies that a VPN connection could be established directly through a specific wireless network 110 to a mobile device 100. The possibility of using a wireless VPN router 75 has only recently been available and could be used when the new Internet Protocol (IP) Version 6 (IPV6) arrives into IP-based wireless networks. This new protocol will provide enough IP addresses to dedicate an IP address to every mobile device 100 and thus make it possible to push information to a mobile device 100 at any time. A principal advantage of using this wireless VPN router 75 is that it could be an off-the-shelf VPN component, thus it would not require a separate wireless gateway 85 and wireless infrastructure 90 to be used. A VPN connection would preferably be a Transmission Control Protocol (TCP)/IP or User Datagram Protocol (UDP)/IP connection to deliver the messages directly to the mobile device 100. If a wireless VPN 75 is not available then a link 95 to the Internet 20 is the most common connection mechanism available and has been described above.

In the automatic redirection system of FIG. 2, a composed e-mail message 15 leaving the e-mail sender 10 arrives at the message server 40 and is redirected by the redirection program 45 to the mobile device 100. As this redirection takes place the message 15 is re-enveloped, as indicated at 80, and a possibly proprietary compression and encryption algorithm can then be applied to the original message 15. In this way,

messages being read on the mobile device 100 are no less secure than if they were read on a desktop workstation such as 35 within the firewall. All messages exchanged between the redirection program 45 and the mobile device 100 preferably use this message repackaging technique. Another goal of this outer envelope is to maintain the addressing information of the original message except the sender's and the receiver's address. This allows reply messages to reach the appropriate destination, and also allows the "from" field to reflect the mobile user's desktop address. Using the user's e-mail address from the mobile device 100 allows the received message to appear as though the message originated from the user's desktop system 35 rather than the mobile device 100.

With reference back to the port 50 and cradle 65 connectivity to the mobile device 100, this connection path offers many advantages for enabling one-time data exchange of large items. For those skilled in the art of personal digital assistants (PDAs) and synchronization, the most common data exchanged over this link is Personal Information Management (PIM) data 55. When exchanged for the first time this data tends to be large in quantity, bulky in nature and requires a large bandwidth to get loaded onto the mobile device 100 where it can be used on the road. This serial link may also be used for other purposes, including setting up a private security key 111 such as an S/MIME or PGP specific private key, the Certificate (Cert) of the user and their Certificate Revocation Lists (CRLs) 60. The private key is preferably exchanged so that the desktop 35 and mobile device 100 share one personality and one method for accessing all mail. The Cert and CRLs are normally exchanged over such a link because they represent a large amount of the data that is required by the device for S/MIME, PGP and other public key security methods.

FIG. 3 depicts a system wherein data transfers 230 between a secure location 220 and a less secure location 240 is managed on a mobile device 100 by a data transfer checker 202. A data transfer checker 202 can be implemented on a mobile device 100 as a software routine or in hardware or firmware. FIG. 4 provides several examples of locations 220 and 240. For example, location 220 may be a top-secret or secure network and location 240 may be an unrestricted network.

As another example, location 220 may be a first application that has received sensitive or confidential information. An attempt to transfer data from the first application to a second application may be prevented by the data transfer checker 202 because if the

data transfer is successful to the second application, then the second application might be used to disseminate the sensitive data to an unsecured location.

FIG. 5 depicts an IT (information technology) administrator 250 (or its agent) providing data transfer criterion or settings 252 to a mobile device 100. The settings 252 can indicate what data transfers 230 are permitted and which ones are not permitted. The settings 252 can be stored in a data store 204 located on the mobile device 100 for access by a data transfer checker 202.

The IT administrator 250 can specify data transfer settings 252 to one or more devices. The settings 252 may be provided to the mobile device 100 over a network (or other data connection mechanism) in order to update the data store 204 on the mobile device 100. The mobile device 100 can be pre-programmed with the settings and can be updated by the IT administrator 250 or can have the initial settings provided by the IT administrator 250.

This provides, among other things, companies with the capability to customize data transfer settings to suit their needs. Also, an IT administrator 250 can provide the same settings to all mobile devices of the company, thereby ensuring that company mobile devices adhere to a consistent IT policy.

An IT policy can be enforced upon mobile devices in many ways, such as through the approaches described in the following commonly assigned United States patent application which is hereby incorporated by reference: "System And Method Of Owner Control Of Electronic Devices" (Serial Number 10/732,132 filed on December 10, 2003). This document illustrates how a user of the mobile device can be prevented from altering or erasing owner control information (e.g., data transfer settings 252) specified by an IT administrator 250.

FIGS. 6 and 7 illustrate a data transfer operational scenario 300. At step 302 in the operational scenario, data transfer settings can be provided to one or more mobile devices by IT administration personnel. A company's IT policy can specify that many different data transfer-related features can be enabled/disabled. As an illustration, the data transfer settings can enable/disable such security-related aspects associated with data transfers as the following:

* whether data forwarding between service books should be allowed.

* whether cut/copy/paste operations between applications should be allowed.

* whether applications should be prevented from opening an internal and an external connection.

* whether IPC (interprocess communication) should be allowed between applications.

Using one or more of these features, the company can help ensure that their private data is kept secure. The data transfer settings are stored at step 304 in one or more data stores that are located on the mobile device.

At step 306, there is an attempt in this operational scenario to transfer data from a first location to a second location. Step 310 retrieves the data transfer settings, and decision step 312 examines whether the data transfer should occur in view of the data transfer settings. If the data transfer should occur as determined by decision step 312, then the data transfer occurs between the first location and the second location, and processing for this operational scenario terminates at end block 320.

However, if decision step 312 determines that the data transfer should not be allowed in view of the settings, then decision step 316 determines whether the user should be notified that the data transfer is not permitted. If the user is not to be notified (e.g., because the settings do not allow a feedback message), then processing for this operational scenario terminates at end block 320. However, if the user is to be notified as determined by decision block 316, then an indication is provided at step 318 to the user that the data transfer is being prevented. Processing for this operational scenario terminates at end block 320.

It should be understood that similar to the other processing flows described herein, the steps and the order of the steps in the flowchart described herein may be altered, modified and/or augmented and still achieve the desired outcome.

FIG. 8 illustrates a data transfer prevention feature mentioned above wherein data transfer 410 between services (400, 420) is prevented. Exemplary services comprise a company email service, a user's personal e-mail service, and an instant messaging service. This data transfer prevention feature allows the company to disable improper forwarding/replying between services. For example, if a user receives an email message via a first service 400, the user is unable to forward it to another email account via a second service 420 (such as a personal e-mail account of the user). Optionally, messages

440 that arrive via a source e-mail server 430 must be replied to or forwarded back through the same source e-mail server 430 from which the message 440 arrived.

FIG. 9 illustrates a data transfer prevention feature mentioned above wherein cut/copy/paste operations 510 are disabled for all or designated applications on the handheld mobile device 100. As an illustration, even if the forwarding between applications or services is disabled, a determined user may copy messages from one application 500, compose a new message in a different application 520 and send it through the different application 520. Disabling cut/copy/paste operations makes this much more difficult for the user to siphon data because they would be forced to retype the entire message or data.

FIG. 10 illustrates a data transfer prevention feature mentioned above wherein Inter-Process Communication (IPC) 710 can be disabled between applications (700, 720) that operate on a mobile device 100. As is known to one skilled in the art, an application may initiate one or more processes in order to accomplish certain tasks on the handheld mobile device 100. This data transfer prevention feature would prevent two malicious applications (700, 720) working together to siphon data. As an example, one application 700 could open up a connection inside the firewall, and another application 720 could open a connection outside the firewall. Then using IPC 710, they could transfer data between the two applications (700, 720) and effectively siphon data. Disabling IPC between the applications (700, 720) prevents this type of attack from occurring.

The data transfer prevention provided by a data transfer checker 202 would inadvertently prohibit IPC between an e-mail program and an address book that are operating on the mobile device 100. Thus, a company can additionally choose which applications are allowed to use IPC, as some applications, such as the e-mail program and the address book, may have a valid use for it.

The systems and methods disclosed herein are presented only by way of example and are not meant to limit the scope of the invention. Other variations of the systems and methods described above will be apparent to those skilled in the art and as such are considered to be within the scope of the invention. For example, the systems and methods disclosed herein may be used with many different computers and devices, such as a wireless mobile communications device shown in FIG. 11. With reference to FIG. 11, the mobile device 100 is a dual-mode mobile device and includes a transceiver 811, a microprocessor 838, a display 822, non-volatile memory 824, random access memory

(RAM) 826, one or more auxiliary input/output (I/O) devices 828, a serial port 830, a keyboard 832, a speaker 834, a microphone 836, a short-range wireless communications sub-system 840, and other device sub-systems 842.

The transceiver 811 includes a receiver 812, a transmitter 814, antennas 816 and 818, one or more local oscillators 813, and a digital signal processor (DSP) 820. The antennas 816 and 818 may be antenna elements of a multiple-element antenna, and are preferably embedded antennas. However, the systems and methods described herein are in no way restricted to a particular type of antenna, or even to wireless communication devices.

The mobile device 100 is preferably a two-way communication device having voice and data communication capabilities. Thus, for example, the mobile device 100 may communicate over a voice network, such as any of the analog or digital cellular networks, and may also communicate over a data network. The voice and data networks are depicted in FIG. 11 by the communication tower 819. These voice and data networks may be separate communication networks using separate infrastructure, such as base stations, network controllers, etc., or they may be integrated into a single wireless network.

The transceiver 811 is used to communicate with the network 819, and includes the receiver 812, the transmitter 814, the one or more local oscillators 813 and the DSP 820. The DSP 820 is used to send and receive signals to and from the transceivers 816 and 818, and also provides control information to the receiver 812 and the transmitter 814. If the voice and data communications occur at a single frequency, or closely-spaced sets of frequencies, then a single local oscillator 813 may be used in conjunction with the receiver 812 and the transmitter 814. Alternatively, if different frequencies are utilized for voice communications versus data communications for example, then a plurality of local oscillators 813 can be used to generate a plurality of frequencies corresponding to the voice and data networks 819. Information, which includes both voice and data information, is communicated to and from the transceiver 811 via a link between the DSP 820 and the microprocessor 838.

The detailed design of the transceiver 811, such as frequency band, component selection, power level, etc., will be dependent upon the communication network 819 in which the mobile device 100 is intended to operate. For example, a mobile device 100 intended to operate in a North American market may include a transceiver 811 designed to

operate with any of a variety of voice communication networks, such as the Mobitex or DataTAC mobile data communication networks, AMPS, TDMA, CDMA, PCS, etc., whereas a mobile device 100 intended for use in Europe may be configured to operate with the GPRS data communication network and the GSM voice communication network. Other types of data and voice networks, both separate and integrated, may also be utilized with a mobile device 100.

Depending upon the type of network or networks 819, the access requirements for the mobile device 100 may also vary. For example, in the Mobitex and DataTAC data networks, mobile devices are registered on the network using a unique identification number associated with each mobile device. In GPRS data networks, however, network access is associated with a subscriber or user of a mobile device. A GPRS device typically requires a subscriber identity module ("SIM"), which is required in order to operate a mobile device on a GPRS network. Local or non-network communication functions (if any) may be operable, without the SIM device, but a mobile device will be unable to carry out any functions involving communications over the data network 819, other than any legally required operations, such as '911' emergency calling.

After any required network registration or activation procedures have been completed, the mobile device 100 may the send and receive communication signals, including both voice and data signals, over the networks 819. Signals received by the antenna 816 from the communication network 819 are routed to the receiver 812, which provides for signal amplification, frequency down conversion, filtering, channel selection, etc., and may also provide analog to digital conversion. Analog to digital conversion of the received signal allows more complex communication functions, such as digital demodulation and decoding to be performed using the DSP 820. In a similar manner, signals to be transmitted to the network 819 are processed, including modulation and encoding, for example, by the DSP 820 and are then provided to the transmitter 814 for digital to analog conversion, frequency up conversion, filtering, amplification and transmission to the communication network 819 via the antenna 818.

In addition to processing the communication signals, the DSP 820 also provides for transceiver control. For example, the gain levels applied to communication signals in the receiver 812 and the transmitter 814 may be adaptively controlled through automatic gain control algorithms implemented in the DSP 820. Other transceiver control algorithms

could also be implemented in the DSP 820 in order to provide more sophisticated control of the transceiver 811.

The microprocessor 838 preferably manages and controls the overall operation of the mobile device 100. Many types of microprocessors or microcontrollers could be used here, or, alternatively, a single DSP 820 could be used to carry out the functions of the microprocessor 838. Low-level communication functions, including at least data and voice communications, are performed through the DSP 820 in the transceiver 811. Other, high-level communication applications, such as a voice communication application 824A, and a data communication application 824B may be stored in the non-volatile memory 824 for execution by the microprocessor 838. For example, the voice communication module 824A may provide a high-level user interface operable to transmit and receive voice calls between the mobile device 100 and a plurality of other voice or dual-mode devices via the network 819. Similarly, the data communication module 824B may provide a high-level user interface operable for sending and receiving data, such as e-mail messages, files, organizer information, short text messages, etc., between the mobile device 100 and a plurality of other data devices via the networks 819.

The microprocessor 838 also interacts with other device subsystems, such as the display 822, the RAM 826, the auxiliary input/output (I/O) subsystems 828, the serial port 830, the keyboard 832, the speaker 834, the microphone 836, the short-range communications subsystem 840 and any other device subsystems generally designated as 842.

Some of the subsystems shown in FIG. 11 perform communication-related functions, whereas other subsystems may provide "resident" or on-device functions. Notably, some subsystems, such as the keyboard 832 and the display 822 may be used for both communication-related functions, such as entering a text message for transmission over a data communication network, and device-resident functions such as a calculator or task list or other PDA type functions.

Operating system software used by the microprocessor 838 is preferably stored in a persistent store such as non-volatile memory 824. The non-volatile memory 824 may be implemented, for example, as a Flash memory component, or as battery backed-up RAM. In addition to the operating system, which controls low-level functions of the mobile device 810, the non-volatile memory 824 includes a plurality of software modules 824A-824N that can be executed by the microprocessor 838 (and/or the DSP 820), including a

voice communication module 824A, a data communication module 824B, and a plurality of other operational modules 824N for carrying out a plurality of other functions. These modules are executed by the microprocessor 838 and provide a high-level interface between a user and the mobile device 100. This interface typically includes a graphical component provided through the display 822, and an input/output component provided through the auxiliary I/O 828, keyboard 832, speaker 834, and microphone 836. The operating system, specific device applications or modules, or parts thereof, may be temporarily loaded into a volatile store, such as RAM 826 for faster operation. Moreover, received communication signals may also be temporarily stored to RAM 826, before permanently writing them to a file system located in a persistent store such as the Flash memory 824.

An exemplary application module 824N that may be loaded onto the mobile device 100 is a personal information manager (PIM) application providing PDA functionality, such as calendar events, appointments, and task items. This module 824N may also interact with the voice communication module 824A for managing phone calls, voice mails, etc., and may also interact with the data communication module for managing e-mail communications and other data transmissions. Alternatively, all of the functionality of the voice communication module 824A and the data communication module 824B may be integrated into the PIM module.

The non-volatile memory 824 preferably also provides a file system to facilitate storage of PIM data items on the device. The PIM application preferably includes the ability to send and receive data items, either by itself, or in conjunction with the voice and data communication modules 824A, 824B, via the wireless networks 819. The PIM data items are preferably seamlessly integrated, synchronized and updated, via the wireless networks 819, with a corresponding set of data items stored or associated with a host computer system, thereby creating a mirrored system for data items associated with a particular user.

Context objects representing at least partially decoded data items, as well as fully decoded data items, are preferably stored on the mobile device 100 in a volatile and non-persistent store such as the RAM 826. Such information may instead be stored in the non-volatile memory 824, for example, when storage intervals are relatively short, such that the information is removed from memory soon after it is stored. However, storage of this information in the RAM 826 or another volatile and non-persistent store is preferred, in

order to ensure that the information is erased from memory when the mobile device 100 loses power. This prevents an unauthorized party from obtaining any stored decoded or partially decoded information by removing a memory chip from the mobile device 100, for example.

The mobile device 100 may be manually synchronized with a host system by placing the device 100 in an interface cradle, which couples the serial port 830 of the mobile device 100 to the serial port of a computer system or device. The serial port 830 may also be used to enable a user to set preferences through an external device or software application, or to download other application modules 824N for installation. This wired download path may be used to load an encryption key onto the device, which is a more secure method than exchanging encryption information via the wireless network 819. Interfaces for other wired download paths may be provided in the mobile device 100, in addition to or instead of the serial port 830. For example, a USB port would provide an interface to a similarly equipped personal computer.

Additional application modules 824N may be loaded onto the mobile device 100 through the networks 819, through an auxiliary I/O subsystem 828, through the serial port 830, through the short-range communications subsystem 840, or through any other suitable subsystem 842, and installed by a user in the non-volatile memory 824 or RAM 826. Such flexibility in application installation increases the functionality of the mobile device 100 and may provide enhanced on-device functions, communication-related functions, or both. For example, secure communication applications may enable electronic commerce functions and other such financial transactions to be performed using the mobile device 100.

When the mobile device 100 is operating in a data communication mode, a received signal, such as a text message or a web page download, is processed by the transceiver module 811 and provided to the microprocessor 838, which preferably further processes the received signal in multiple stages as described above, for eventual output to the display 822, or, alternatively, to an auxiliary I/O device 828. A user of mobile device 100 may also compose data items, such as e-mail messages, using the keyboard 832, which is preferably a complete alphanumeric keyboard laid out in the QWERTY style, although other styles of complete alphanumeric keyboards such as the known DVORAK style may also be used. User input to the mobile device 100 is further enhanced with a plurality of auxiliary I/O devices 828, which may include a thumbwheel input device, a

touchpad, a variety of switches, a rocker input switch, etc. The composed data items input by the user may then be transmitted over the communication networks 819 via the transceiver module 811.

When the mobile device 100 is operating in a voice communication mode, the overall operation of the mobile device is substantially similar to the data mode, except that received signals are preferably be output to the speaker 834 and voice signals for transmission are generated by a microphone 836. Alternative voice or audio I/O subsystems, such as a voice message recording subsystem, may also be implemented on the mobile device 100. Although voice or audio signal output is preferably accomplished primarily through the speaker 834, the display 822 may also be used to provide an indication of the identity of a calling party, the duration of a voice call, or other voice call related information. For example, the microprocessor 838, in conjunction with the voice communication module and the operating system software, may detect the caller identification information of an incoming voice call and display it on the display 822.

A short-range communications subsystem 840 is also included in the mobile device 100. The subsystem 840 may include an infrared device and associated circuits and components, or a short-range RF communication module such as a Bluetooth™ module or an 802.11 module, for example, to provide for communication with similarly-enabled systems and devices. Those skilled in the art will appreciate that "Bluetooth" and "802.11" refer to sets of specifications, available from the Institute of Electrical and Electronics Engineers, relating to wireless personal area networks and wireless local area networks, respectively.

The systems' and methods' data may be stored in one or more data stores. The data stores can be of many different types of storage devices and programming constructs, such as RAM, ROM, Flash memory, programming data structures, programming variables, etc. It is noted that data structures describe formats for use in organizing and storing data in databases, programs, memory, or other computer-readable media for use by a computer program.

The systems and methods may be provided on many different types of computer-readable media including computer storage mechanisms (e.g., CD-ROM, diskette, RAM, flash memory, computer's hard drive, etc.) that contain instructions for use in execution by a processor to perform the methods' operations and implement the systems described herein.

The computer components, software modules, functions and data structures described herein may be connected directly or indirectly to each other in order to allow the flow of data needed for their operations. It is also noted that a module or processor includes but is not limited to a unit of code that performs a software operation, and can be implemented for example as a subroutine unit of code, or as a software function unit of code, or as an object (as in an object-oriented paradigm), or as an applet, or in a computer script language, or as another type of computer code. The software components and/or functionality may be located on a single computing device or distributed across multiple computing devices depending upon the situation at hand.

CLAIMS:

1. A method of handling data transfers on a device, comprising:

receiving a data transfer request to transfer data from a first location to a second location;

wherein the first location is more secure than the second location;

retrieving data transfer settings from a data store responsive to receiving the data transfer request;

wherein the data transfer settings indicate whether a data transfer is to occur based upon a security-related aspect associated with the data transfer;

determining whether to transfer the data from the first location to the second location based upon the data transfer settings;

wherein the data is transferred responsive to the determining step.

2. The method of claim 1, wherein the data transfer security-related aspect includes an aspect selected from the group comprising: level of security associated with destination of the data transfer; type of communication operation to be performed between the first location and the second location; and combinations thereof;

wherein the type of data transfer communication operation includes an operation selected from the group comprising: data forwarding between service books; opening an internal and an external connection; an Inter-Process Communication (IPC) between applications; a cut-copy-paste type operation between applications; and combinations thereof;

wherein a notification is provided to a user interface of the device to indicate that the data transfer request was not completed because of the determining step.

3. The method of claim 1, further comprising:

receiving the data transfer settings from an administrator; and

storing the data transfer settings in a data store, responsive to receiving the data transfer settings from the administrator.

4. The method of claim 1, wherein the first location is a first application, and the second location is a second application.

5. The method of claim 1, wherein the first location is a first service, and the second location is a second service.

6. The method of claim 5, wherein the first and second services are selected from a group of services comprising: a personal electronic mail service, a professional electronic mail service, or an instant messaging service.

7. The method of claim 1, wherein the determining step that is performed based upon the data transfer settings prevents a malicious application from siphoning data contained inside a corporation's or government's firewall to outside the firewall.

8. The method of claim 1, wherein the first location is a first memory associated with the device, and the second location is a second memory located on another device.

9. The method of claim 1, wherein the first location and second location correspond to companies or governments that have different types of networks with different levels of security.

10. The method of claim 1, wherein the device is a mobile wireless communications device.

11. The method of claim 1, wherein the data transfer settings are configured to prevent data transfers using Inter-Process Communications (IPC).

12. The method of claim 11, wherein a company or government that owns the device sets the data transfer settings to choose which applications are permitted to use IPC for data transfers.

13. The method of claim 1, wherein the data transfer settings indicate what data transfers are permitted and which data transfers are not permitted.

14. The method of claim 1, further comprising:

receiving updated data transfer settings from an information technology (IT) administrator; and

replacing the data transfer settings in the data store located on the device with the updated data transfer settings.

15. The method of claim 14, wherein the IT administrator of a company or government that owns the device customizes the data transfer settings in accordance with the company's or government's policy requirements.

16. The method of claim 15, wherein the IT administrator provides the same settings to multiple devices owned by the company or the government, thereby ensuring that company or government mobile devices adhere to a consistent IT policy.

17. The method of claim 14, wherein the IT administrator can specify at least data transfer settings selected from one or more of the following policies: whether data forwarding between service books should be allowed; whether cut-copy-paste operations between applications should be allowed; whether applications should be prevented from opening an internal and an external connection; whether Inter-Process Communication (IPC) should be allowed between applications; and combinations thereof.

18. Computer software stored on one or more computer readable media, the computer software comprising program code for carrying out a method according to claim 1.

19. A data transfer apparatus for transferring data on a device from a first location to a second location, the apparatus comprising:

a data store that stores data transfer settings;

wherein the data transfer settings indicate whether a data transfer is to occur based upon a security-related aspect associated with the data transfer;

a data transfer checker that is configured to retrieve data transfer settings from the data store responsive to the device receiving a request to transfer data from the first location to the second location;

wherein the data transfer checker is configured to prevent the request from being performed responsive to the data transfer settings.

20. A data transfer system for transferring data on a wireless mobile communications device from a first location to a second location, the system comprising:

means for receiving a data transfer request to transfer data from a first location to a second location;

wherein the first location is more secure than the second location;

means for retrieving data transfer settings from a data store responsive to receiving the data transfer request;

wherein the data store is located on the wireless mobile communications device;

wherein the data transfer settings indicate whether a data transfer is to occur based upon a security-related aspect associated with the data transfer;

wherein the data transfer is a transfer selected from the group comprising: data forwarding between service books; a cut-copy-paste operation between applications; applications opening an internal and an external connection; IPC (interprocess communication) between applications;

means for determining whether to transfer the data from the first location to the second location based upon the data transfer settings;

wherein the data is transferred responsive to the determining of whether to transfer the data from the first location to the second location based upon the data transfer settings.

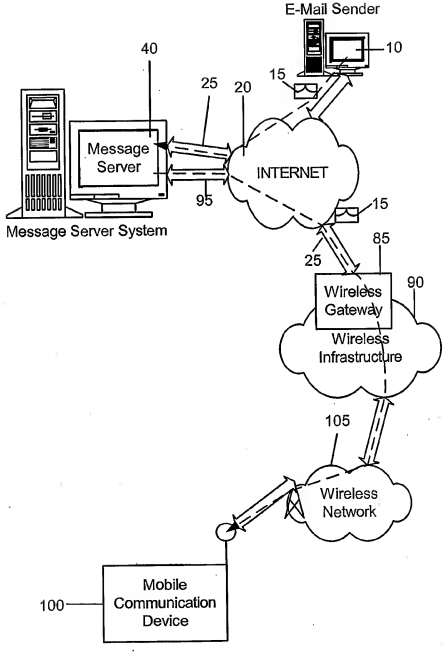

E-Mail Sender
10
40
25
20
15
Message Server
INTERNET
95
15
Message Server System
85
25
90
Wireless Gateway
Wireless Infrastructure
105
Wireless Network
Mobile Communication Device
100

FIG. 1

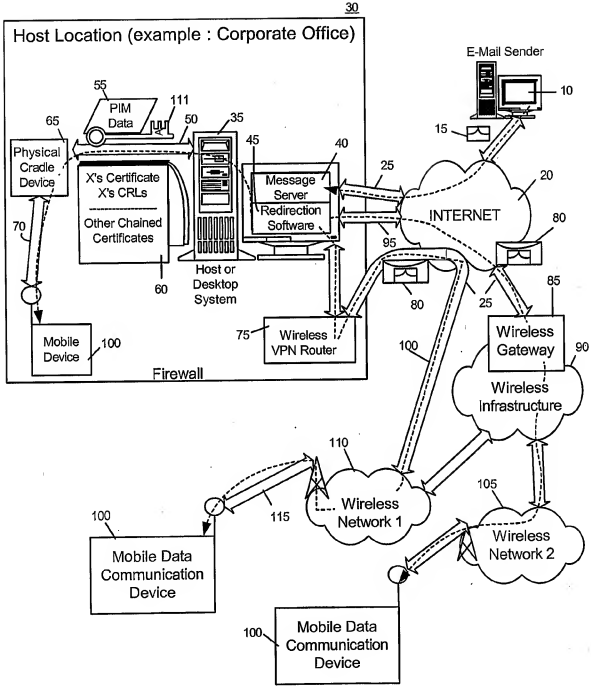

30
Host Location (example : Corporate Office)
E-Mail Sender
10
55
PIM Data
111
65
50
35
45
40
15
Physical Cradle Device
X's Certificate
X's CRLs
Other Chained Certificates
Message Server
Redirection Software
25
20
INTERNET
70
95
80
60
Host or Desktop System
85
Mobile Device
100
75
Wireless VPN Router
Firewall
Wireless Gateway
90
Wireless Infrastructure
110
105
Wireless Network 1
Wireless Network 2
115
Mobile Data Communication Device
Mobile Data Communication Device

FIG. 2

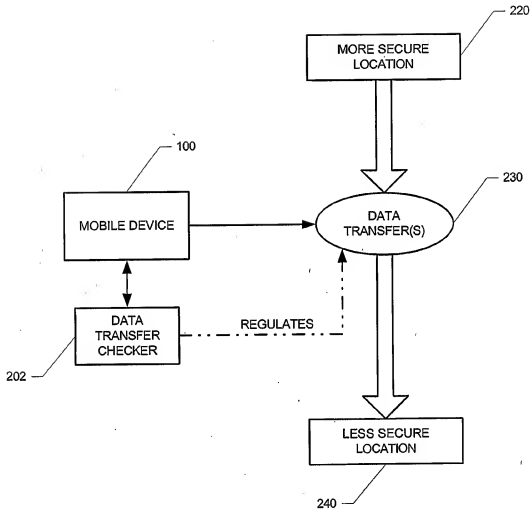

220
MORE SECURE LOCATION
100
MOBILE DEVICE
230
DATA TRANSFER(S)
DATA TRANSFER CHECKER
REGULATES
202
LESS SECURE LOCATION
240

FIG. 3

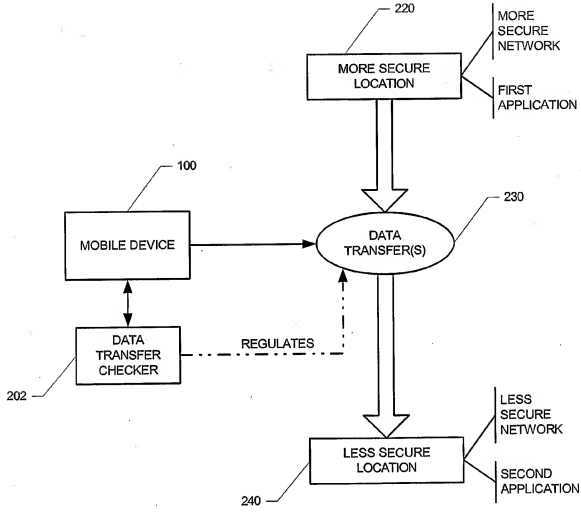

220
MORE SECURE NETWORK
MORE SECURE LOCATION
FIRST APPLICATION
100
230
MOBILE DEVICE
DATA TRANSFER(S)
DATA TRANSFER CHECKER
REGULATES
202
LESS SECURE NETWORK
LESS SECURE LOCATION
SECOND APPLICATION
240

FIG. 4

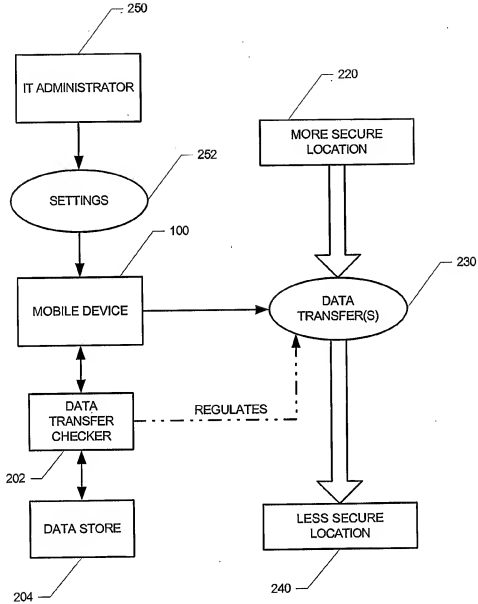

250
IT ADMINISTRATOR
220
MORE SECURE LOCATION
252
SETTINGS
100
230
MOBILE DEVICE
DATA TRANSFER(S)
DATA TRANSFER CHECKER
REGULATES
202
DATA STORE
LESS SECURE LOCATION
204
240

FIG. 5

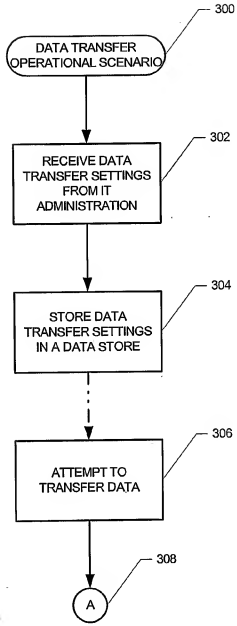

300
DATA TRANSFER OPERATIONAL SCENARIO
302
RECEIVE DATA TRANSFER SETTINGS FROM IT ADMINISTRATION
304
STORE DATA TRANSFER SETTINGS IN A DATA STORE
306
ATTEMPT TO TRANSFER DATA
308
A

FIG. 6

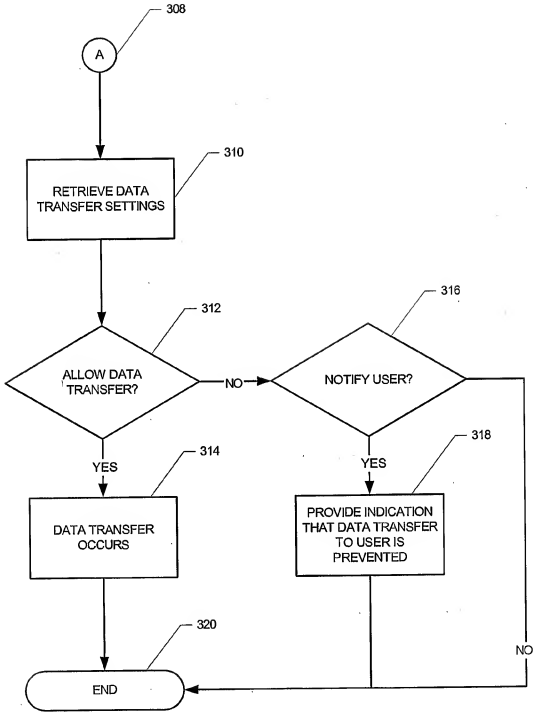

308
A
310
RETRIEVE DATA TRANSFER SETTINGS
312
ALLOW DATA TRANSFER?
NO
316
NOTIFY USER?
YES
314
DATA TRANSFER OCCURS
YES
318
PROVIDE INDICATION THAT DATA TRANSFER TO USER IS PREVENTED
NO
320
END

FIG. 7

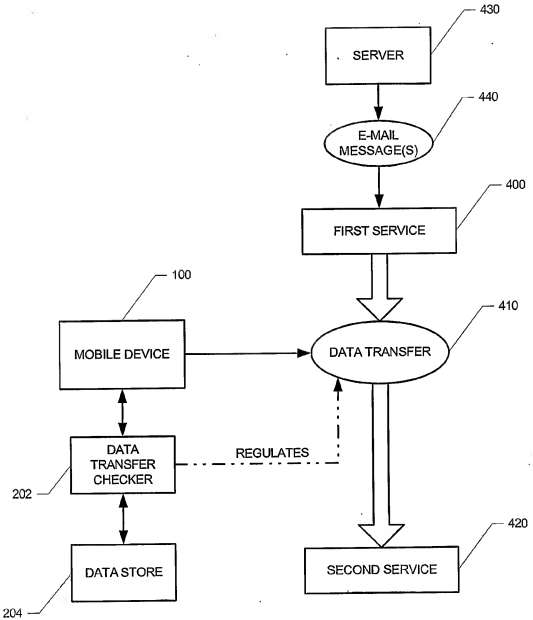

430
SERVER
440
E-MAIL MESSAGE(S)
400
FIRST SERVICE
100
410
MOBILE DEVICE
DATA TRANSFER
DATA TRANSFER CHECKER
REGULATES
202
420
SECOND SERVICE
DATA STORE
204

FIG. 8

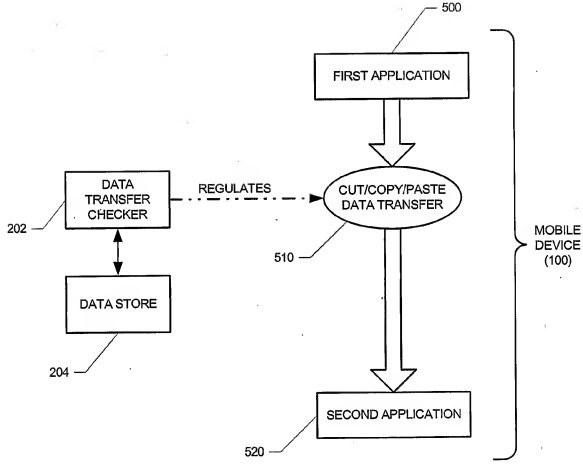

500
FIRST APPLICATION
DATA TRANSFER CHECKER
REGULATES
CUT/COPY/PASTE DATA TRANSFER
202
510
MOBILE DEVICE (100)
DATA STORE
204
SECOND APPLICATION
520

FIG. 9

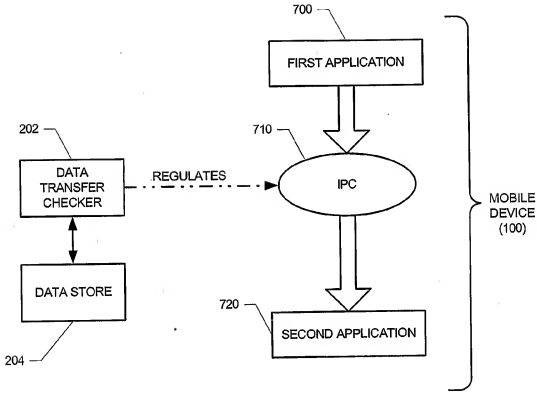

700
FIRST APPLICATION
202
710
DATA TRANSFER CHECKER
REGULATES
IPC
MOBILE DEVICE (100)
DATA STORE
720
SECOND APPLICATION
204

FIG. 10

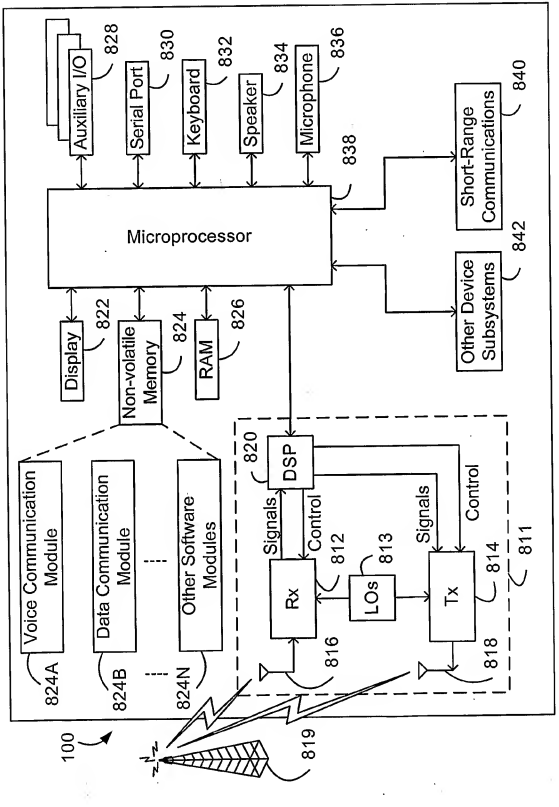

100
819
Voice Communication Module
824A
Data Communication Module
824B
Other Software Modules
824N
Display
822
Non-volatile Memory
824
RAM
826
Microprocessor
838
Auxiliary I/O
828
Serial Port
830
Keyboard
832
Speaker
834
Microphone
836
Short-Range Communications
840
Other Device Subsystems
842
820
DSP
Signals
Control
812
Rx
LOs
813
Signals
Control
814
Tx
811
816
818

FIG. 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2005/000652

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7): H04L 9/32, H04L 12/22, H04Q 7/20

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(7): H04L 9/32, H04L 12/22, H04Q 7/20 (using keywords)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
WEST, Canadian Patent Database, Delphion
Keywords: mobile wireless communications, data transfer, secure, checker, blocker, prevention, control, e-mail, IPC, siphoning, administrator

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US2003/0226015, "Method and Apparatus for Configuring Security Options in a Computer System", Neufeld et al. (2003-12-04) [0022], [0077], [0084] and Tables 1 to 4, [0090], [0091]	1 - 20
A	US2003/0236983, "Secure Data Transfer in Mobile Terminals and Methods Therefor", Mihm, T. (2003-12-25) [0028], [0032], [0034], [0035], [0047], [0048], [0058] to [0060]	1 - 20
A	US2003/0026220, "Stystem and Related Methods to Facilitate Delivery of Enhanced Data Services in a Mobile Wireless Communications Environment", Uhlik et al. (2003-02-06) [0022], [0026] and Fig. 1, [0098] and Fig. 10	1 - 20

[ ] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18-July 2005 (18-07-2005)	17 August 2005 (17-08-2005)
Name and mailing address of the ISA/CA Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001(819)953-2476	Authorized officer Lawrence J. Engel (819) 997-2936

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/CA2005/000652

Patent Document Publication Cited in Search Report	Date	Patent Family Member(s)	Publication Date
US2003226015	04-12-2003	US2003226015 A1	04-12-2003
US2003026220	06-02-2003	US2003026220 A1	06-02-2003
US2003236983	25-12-2003	AU2003225251 A1	06-01-2004
		US2003236983 A1	25-12-2003
		WO2004002054 A1	31-12-2003